I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Protecting Our Digital Walls: Regulating the Privacy Policy Changes Made by Social Networking Websites

ROBERT E. LEMONS*

Abstract: Online social networking websites, such as Facebook, are growing in both size and popularity. These sites operate on the basic idea that users should openly share personal information with each other. The vast majority of this information is both personally identifiable and private in nature, generating a host of privacy concerns. One easily overlooked issue is how social networking sites, themselves, change their privacy policies after users have already shared personal information, fundamentally altering the way users can control their own information. After exploring the growth of online social networking and the increase in user dissatisfaction with social network privacy policy changes, this Note argues that federal regulation could help to create transparency and protect users against unanticipated changes in their ability to control their information. This Note also discusses the apparent disconnect between users' privacy preferences and actual online behavior, exploring why this disconnect exists and its implications for the effectiveness of potential regulation.

---

* Robert E. Lemons is a 2011 J.D. candidate at The Ohio State University Moritz College of Law. He is also an active user of online social networking sites, including Facebook. He would like to thank Professors Peter Shane and Dennis Hirsch for their thoughtful guidance. He would also like to thank his family for their continued support.

INTRODUCTION

Imagine the window in the front of your house or apartment. As long as the shades are open, any passerby can look in, getting a small glimpse of what you keep inside. However, the walls of your house keep people on the outside from getting a complete look at what you, most likely, consider private. This was the truth when you bought the house or rented the apartment. At that time, you were completely aware of the nature of your privacy and could make choices about what to keep in front of an open window and what to keep behind a wall. Now imagine that you wake up one morning to find that you now have the ability to control who can look into your open windows. No one gets to peek through if you do not want them to. However, in exchange for this privacy enhancement, the walls of your living room, kitchen, and closets are now see-through and anyone passing by is free to look. While a far-fetched situation, this is analogous to how one popular social networking site, Facebook, reorganized its privacy policy at the tail end of 2009 by permanently exposing information that users were previously able to keep private.[1]

As the operators of social networks are not likely to introduce restrictive privacy options that could cripple their own sites, future privacy changes will likely favor the networks themselves. A method of regulation needs to be implemented in order to make sure that the proper balance between privacy and openness on social networks is maintained, and to make sure that social network operators do not quickly and drastically alter their privacy policies with little notice or input from the users.

Part I of this note will examine the rise of social networks and their history of controversial privacy policy changes, focusing primarily on Facebook (the largest online social networking site in the world). Part II will propose a governmental regulation board to oversee future privacy policy changes on social networks. Part III will discuss possible concerns and limitations of implementing a governmental review of social network privacy changes.

---

[1] Details of Facebook's December 2009 privacy changes can be found in Part I of this Note.

I. AN EXPLORATION OF THE HISTORY OF ONLINE SOCIAL NETWORKING WEBSITES AND RECENT USER BACKLASH OVER PRIVACY CHANGES

With the spread of social networking sites showing no signs of slowing, the potential impact on personal privacy expands on a daily basis.[2] In order to understand the importance of privacy on these networks and why the change of privacy options can lead to concern, it is important to look first at the history of social networking sites as well as the history of their privacy changes.

A. A (BRIEF) HISTORY OF ONLINE SOCIAL NETWORKING WEBSITES

What is an online social network? There is no formal definition to describe these fast growing digital networks. Nicole Ellison and danah boyd, social network researchers, describe social networks as:

> "[W]eb-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[3]

These networks often contain visible profiles and a list of "friends" within the same network.[4] The profiles of any particular user can contain information pertaining to age, location, interests, and any other general or specific information about a user, that the user wishes to include, which can be used to create an "about me" section.[5] Most online social networking sites also encourage users to upload a personal photograph.[6] Users of these sites are encouraged to identify others on the site in order to establish "friends," although Ellison and

---

[2] *Led by Facebook, Twitter, Global Time Spend on Social Media Sites up 82% Year over Year*, NIELSENWIRE (Jan. 22 2010), http://blog.nielsen.com/nielsenwire/global/led-by-facebook-twitter-global-time-spent-on-social-media-sites-up-82-year-over-year/.

[3] danah boyd & Nicole Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 211 (2008).

[4] *Id.*

[5] *Id.* at 213.

[6] *Id.*

boyd note that the term may not mean "friendship in the everyday vernacular sense," due to the varied reasons that people "connect" with each other.[7]

Social networking sites generally provide users with discretion over how visible their personal pages are.[8] In the everyday course of using a social networking site, users can often "traverse the network" by clicking through friend lists.[9] Further, social networks often provide users with the ability to post comments on another user's page, send private messages to other users, post personal videos, send instant messages, and perform various other communication tasks.[10]

According to Ellison and boyd, the first web service that meets their definition of online "social network," SixDegrees.com, was created in 1997.[11] Over the next four years, many other online social networking sites began to launch worldwide, catering to many diverse groups.[12] "Some of these early sites have since closed,"[13] ushering the way for newer ones. In 2003, online social networks began going mainstream, attracting significant attention and a large number of users.[14] Examples of the kinds of networks that emerged during this era include the popular online social networking sites MySpace and Facebook.[15]

B. RECENT USER BACKLASH OVER FACEBOOK'S PRIVACY CHANGES

Because a comprehensive review of privacy changes across all social networks is all but impossible, I will focus on the largest and

---

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.* at 213 – 214.

[11] *Id.* at 214 (The authors explain: "SixDegrees.com allowed users to create profiles, list their Friends and, beginning in 1998, surf the Friends lists.").

[12] *Id.*

[13] James Grimmelmann, *Saving Facebook*, 94 Iowa L. Rev. 1137, 1144 (2009).

[14] boyd & Ellison, *supra* note 4, at 216.

[15] For a more detailed history of online social networking sites, please *see Id.* at 214 – 219.

fastest growing[16] online social networking website, Facebook.[17] There can be no doubt that Facebook has emerged as the dominant social networking site globally. By October 2010, Facebook had more than 500 million active users.[18] This is essentially the populations of the United States, Germany, and Japan, combined.[19] The rapid expansion of users has made Facebook the "biggest information network on the internet."[20] Each user of Facebook has the option of continually updating his or her "status," a brief message that typically broadcasts what the user is thinking or doing. Users currently update these messages more than 60,000,000 times daily and upload more than three billion photographs each month.[21] Further, Facebook provides more than seventy translations of its content, which is helpful because about 70 percent of its users are located outside the United States.[22] Because Facebook has emerged as the dominant online social network,[23] the changes that it makes to its privacy policy and the methods through which it implements these changes tend to receive widespread public notice.

Since its inception in 2004, Facebook has been no stranger to controversy surrounding its rapidly changing, and sometimes unannounced, privacy policies. On September 5, 2006, Facebook

---

[16] *Facebook Largest Social Network and Fastest Growing*, ACCURACAST (Aug. 15, 2008), http://www.accuracast.com/search-daily-news/social-media-7471/facebook-largest-social-network-and-fastest-growing/.

[17] *Facebook*, http://www.facebook.com (lasted visited Mar. 14, 2011).

[18] *Facebook Press Room Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Mar. 14, 2011).

[19] Cecilia Kang, *Facebook to hit 500 million users,* but *meteoric rise has come with growing pains*, WASH. POST (July 19, 2010), http://voices.washingtonpost.com/posttech/2010/07/facebook_hits_500_million_user.html.

[20] *Id.*

[21] *Facebook*, *supra* note 19.

[22] *Id.*

[23] In fact, besides being the world's largest online social network, Facebook has, on occasion, become the most viewed website in the United States. Heather Dougherty, *Facebook Reaches Top Ranking in US*, EXPERIAN HITWISE (Mar. 15, 2010), http://weblogs.hitwise.com/heather-dougherty/2010/03/facebook_reaches_top_ranking_i.html.

unveiled its "news feed" and "mini feed" features.[24] These new features served to aggregate the activities of a user and post them on the user's page as well as broadcast them to the user's friends.[25] Less than a day after introducing the new features, Facebook received thousands of emails from users claiming the feature invaded privacy.[26] Facebook groups against the changes were created, petitions to have the changes reversed were circulated, and boycotts of Facebook were planned.[27] As a result of this backlash, arguably prompted by the fact that many users had regarded Facebook as a social network that valued and protected user privacy,[28] Facebook changed its privacy controls to allow users to decide what could be posted in the feeds.[29]

Before long, however, Facebook again antagonized its users. On November 6, 2007, Facebook launched its Beacon program.[30] Facebook described Beacon as a "core element of the Facebook Ads system for connecting businesses with users and targeting advertising to the audiences they want."[31] The program reported information about Facebook users' activities on third party sites back to Facebook and posted details of a user's activities on that user's profile.[32] The kind of activities that Beacon reported include "posting an item for

---

[24] Sarah Lacy, *Facebook Learns from Its Fumble*, BUS. WK. (Sept. 8, 2006), http://www.businessweek.com/technology/content/sep2006/tc20060908_536553.htm.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Leading Websites Offer Facebook Beacon for Social Distribution*, FACEBOOK (Nov. 6, 2007), http://www.facebook.com/press/releases.php?p=9166.

[31] *Id.*

[32] *Id.* For example, Fandango, a website catered to moviegoers and a participant in the Beacon program, would post information about movie ticket purchases by any Facebook user on that user's wall in an effort to let users further demonstrate their movie interests to their friends (and no doubt further promote the Fandango brand by increased awareness). At Beacon's inception, there were 44 websites participating including popular companies such as Blockbuster, the New York Times, the NBA, Sony, and CBS).

sale, completing a purchase, scoring a high score in an online game or viewing of video."[33]

Shortly after the Beacon program was implemented, a Facebook group was formed as a petition to get Facebook to cease the program.[34] This group, which today still has more than 73,000 members, cited privacy concerns as its core objection to the program.[35] Users specifically objected to the automatic sharing of details regarding user purchases on other sites.[36]

As a response to the harsh user reaction, Facebook changed its Beacon program from opt-out (meaning users would have to proactively un-register themselves from it) to opt-in (meaning that users would have to confirm to Facebook, on each individual instance, whether or not they wanted their information from third party sites to be broadcast on Facebook).[37] Amidst concerns that Facebook was still collecting user information despite the policy change,[38] Facebook officially changed the Beacon program to allow users to opt-out of it entirely.[39] The controversy over the Beacon program and its implications to Facebook users' privacy culminated in a class action suit brought against Facebook and its third party partners.[40] Facebook

---

[33] *Id.*

[34] *Petition: Facebook, stop invading my privacy!*, FACEBOOK, http://www.facebook.com/group.php?gid=5930262681 (last visited Mar. 14, 2011).

[35] *Id.*

[36] *Id.*

[37] Dan Farber, *Facebook Beacon update: No activities published without users proactively consenting*, ZDNET (Nov. 29, 2007, 19:05), http://blogs.zdnet.com/BTL/?p=7188/.

[38] Juan Carlos Perez, *Facebook's Beacon More Intrusive Than Previously Thought*, PCWORLD (Nov. 30, 2007), http://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html.

[39] Mark Zuckerberg, *Thoughts on Beacon*, FACEBOOK (Dec. 5, 2007, 09:00), http://blog.facebook.com/blog.php?post=7584397130.

[40] Nancy Gohring, *Facebook faces class-action suit over Beacon*, NETWORK WORLD (Aug. 13, 2008), http://www.networkworld.com/news/2008/081308-facebook-faces-class-action-suit-over.html.

eventually settled the suit in September 2009 and agreed to shut down the Beacon program.[41]

In February 2009, Facebook made unannounced changes to its Terms of Use without anyone widely noticing until weeks later.[42] The changes effectively gave Facebook permission to use the content that users posted on its site forever, regardless of whether or not the user maintained an open account.[43] The change prompted user backlash and a federal complaint by the Electronic Privacy Information Center (EPIC). [44]

Facebook quickly reverted back to its old Terms of Service.[45] It then began soliciting user input on new privacy changes.[46] As part of this solicitation, Facebook gave users one month to comment on the proposed terms of service changes.[47] The outreach process also included virtual town hall meetings to allow users to comment on the proposed changes.[48] Facebook promised that the new Terms of Service would be binding if thirty percent of active users participated

---

[41] Eric Eldon, *Facebook Settles Beacon Case: No More Beacon, But There's a $9.5M "Privacy Fund,"* INSIDE FACEBOOK (Sept. 18, 2009), http://www.insidefacebook.com/2009/09/18/facebook-settles-beacon-case-no-more-beacon-but-theres-a-9-5m-privacy-fund/.

[42] JR Raphael, *Facebook Privacy Change Sparks Federal Complaint*, PCWORLD (Feb. 17, 2009, 17:37), http://www.pcworld.com/article/159703/facebook_privacy_change_sparks_federal_complaint.html?tk=rel_news/.

[43] Chris Walters, *Facebook's New Terms of Service: "We Can Do Anything We Want With Your Content. Forever,"* THE CONSUMERIST (Feb. 15, 2009), http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html.

[44] *See supra* note 43.

[45] Ben Popken, *Facebook Reverts Back To Old Terms Of Service*, THE CONSUMERIST (Feb. 18, 2009), http://consumerist.com/2009/02/facebook-reverts-back-to-old-terms-of-service.html.

[46] Josh MacFadden, *Facebook Soliciting User Input On Policies*, CREATIVITY LIFE CYCLES (Feb. 26, 2009), http://www.etrademarkagent.com/2009/02/articles/trademarks-in-the-news/facebook-soliciting-user-input-on-policies/.

[47] *Id.*

[48] Daniel Ionescu, *Rewriting Facebook's Terms of Service*, PCWORLD (Feb. 27, 2009), http://www.pcworld.com/article/160358/rewriting_facebooks_terms_of_service.html.

in a vote to ratify them.[49] This new method of developing policy on social networks was heralded as "a revolutionary move toward democratic social networking"[50] and as a "democratic move" that would give its members an "unprecedented voice."[51] This praise for Facebook, however, would not last long.

In December 2009, Facebook adopted a new privacy policy[52] that has been labeled as "Facebook's Great Betrayal."[53] Information that users could previously keep private was permanently exposed. Users no longer had the ability to control who could view their friends list, profile pictures, fan pages, and affiliations with various Facebook-enabled subnetworks.[54] While Facebook, after making the changes, prompted all users to update their privacy settings, most of the default choices that Facebook recommended were to allow everyone to view your information or let your friends and their friends view your information.[55] As a result of the privacy change, even previously private photos of Facebook's CEO, Mark Zuckerberg, were made public.[56]

---

[49]Tom Spring, *Dawn of a Facebook Democracy? Users Invited to Shape Site's Policies*, PCWORLD (Feb. 26, 2009), http://www.pcworld.com/article/160314/dawn_of_a_facebook_democracy_users_invited_to_shape_sites_policies.html?tk=rel_news.

[50] Ionescu, *supra* note 49.

[51] Edward Baig, *In democratic move, Facebook seeks user input on policies*, USA TODAY (Feb. 27, 2009), http://www.usatoday.com/tech/news/2009-02-26-facebook_N.htm.

[52] This privacy policy does not appear to be related in any way to the democratic process proposed by Facebook in February of 2009. It appears as if that vote did not garner the thirty percent active user vote required, which is not especially surprising as that would have required, at the time, nearly 60 million users to vote on the privacy changes. *See* JR Raphael, *Facebook Opens the Polls for Privacy Policy Vote*, PCWORLD (Apr. 17, 2009, 8:28 AM), http://www.pcworld.com/article/163322/facebook_opens_the_polls_for_privacy_policy_vote.html.

[53] Ryan Tate, *Facebook's Great Betrayal*, GAWKER (Dec. 14, 2009), http://gawker.com/5426176/facebooks-great-betrayal.

[54] *Id.*

[55] *Id.*

[56] Ryan Tate, *Facebook CEO's Private Photos Exposed by the New 'Open' Facebook*, GAWKER (Dec. 11, 2009), http://gawker.com/5423914/facebook-ceos-private-photos-exposed-by-the-new-open-facebook/gallery/.

II. A PROPOSAL TO REGULATE ONLINE SOCIAL NETWORKING WEBSITE PRIVACY POLICY CHANGES

As illustrated by the Facebook examples, the very nature of a social network[57] creates an enormous number of privacy issues. James Grimmelmann, an associate professor of law at New York Law School, believes that the privacy changes made by Facebook are unpredictable and privacy threatening.[58] Grimmelmann additionally believes that, when sites such as Facebook enact these changes unilaterally, it is questionable whether or not users are ever giving their consent.[59] To Grimmelmann, operators of social networking sites in the United States are relatively free of accountability for privacy policy changes because "the lack of a comprehensive information-privacy statute means that [a social networking site] needs no permission in the first place to collect personal data."[60]

There are no laws or regulations that directly address how privacy on social networks should be implemented or revised. Moreover, there is no preventative protection of the privacy interests of the users of online social networking sites that would stop massive policy changes from quickly occurring. Once a social networking site decides to change its privacy policy, there is nothing requiring advance notice of the change or transparency in the process. Because of the lack of any comprehensive information privacy law, people concerned with their privacy on social networks appear to be attempting to form piecemeal protection utilizing existing laws to address their concerns.[61]

The Electronic Privacy Information Center ("EPIC"), a public interest research center that focuses attention on civil liberties issues,[62] filed complaints with the Federal Trade Commission ("FTC")

---

[57] Users voluntarily share information with the promise of some control over its dissemination.

[58] Grimmelmann, *supra* note 14, at 1201.

[59] *Id.*

[60] *Id.*

[61] The recent case against the Facebook Beacon program included counts that Facebook violated sections of the Electronic Communications Privacy Act, Violation of Computer Fraud and Abuse Act, Violation of Video Privacy Protection Act, and other California State consumer protection laws. A copy of the complaint is available at

[62] *About EPIC*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/epic/about.html (last visited Mar. 14, 2011).

over Facebook's December 2009 privacy changes.[63] The complaint alleges that the new Facebook privacy policies "violate user expectations, diminish user privacy, and contradict Facebook's own representations."[64] The complaint further alleges that these violations constitute unfair and deceptive business practices under Section 5 of the Federal Trade Commission Act ("FTCA").[65]

Section 5 of the FTCA declares that unfair methods of competition and deceptive business practices are unlawful.[66] It invests the FTC with the authority to prevent businesses from engaging in these acts.[67] The FTC has been using this authority to protect personal information on internet websites. The Commission describes a "key part" of its privacy program as "making sure companies keep the promises they make to consumers about privacy, including the precautions they take to secure consumers' personal information."[68] According to the FTC, under Section 5, it has "brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information."[69] Once such case involved the social networking service Twitter,[70] where the FTC challenged the service by alleging that the service deceived its users by not honoring the users' choice to keep certain site postings private.[71]

---

[63] *In re Facebook*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/inrefacebook (last visited Mar. 14, 2011).

[64] Complaint available at: http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf

[65] *Id.*

[66] Unfair methods of competition unlawful; prevention by Commission, 15 U.S.C. §45 (2006).

[67] *Id.*

[68] *Enforcing Privacy Promises: Section 5 of the FTC Act*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/privacy/privacyinitiatives/promises.html (last visited Mar. 14, 2011).

[69] *Id.*

[70] Twitter is a social networking platform that allows users to share short communications, referred to as "tweets," of 140 characters or less. *See Twitter*, http://twitter.com/about (last visited Mar. 14, 2011).

[71] *See In re Twitter, Inc.*, No. 092-3093, 2010 WL 2638509 (F.T.C. June 24, 2010) (proposed consent order).

Existing laws, however, are not efficiently addressing the concerns of privacy changes on social networks. The FTC currently has the power to investigate whether websites are honoring their own privacy policies, but only after privacy statements and security have been changed or circumvented. Further, it is not clear what can be done when a site, such as Facebook, drastically alters its privacy policy without any actual details of the new policy being disseminated ahead of the change.

Unfortunately in the case of social networks, where people invest a lot of their own personal information in an effort to expand the network, once the proverbial cat is out of the "privacy bag," it can't be put back in; when something considered private is exposed to the public, it is difficult or impossible to re-privatize. There need to be protections put into place to ensure that social networking sites cannot fundamentally alter their privacy policies without any real notice and without giving network users time to consent to the changes or otherwise remove information that they do not want to be disclosed.

The Beacon case settled out of court before any ruling on the claims could be given.[72] This leaves it uncertain as to whether a court would find that existing laws cover the scope of social network privacy. The EPIC complaint is too recent to have any known effect.[73] Further, the social networks themselves should not have to operate in fear of a lawsuit every time they decide that a privacy policy update is needed. This could stop the evolution of privacy policies of social networks, which concededly must be allowed to adapt to society's concerns and the technological advances that are made on the networks.

Grimmelmann believes that sites such as Facebook need to become more predictable in the way they change their privacy policies.[74] The FTC has recognized that, had companies such as Facebook conducted a more thorough privacy review before launching their privacy changes, they may have been able to avoid any user

---

[72] Jon Brodkin, *Facebook Halts Beacon, Gives $9.5 M to Settle Lawsuit*, PCWORLD (Dec. 8, 2009), http://www.pcworld.com/article/184029/facebook_halts_beacon_gives_95m_to_settle_lawsuit.html.

[73] However, the FTC has indicated an interest in investigating Facebook's privacy changes. *See supra* note 62.

[74] Grimmelmann, *supra* note 14, at 1200.

backlash they received.[75] However, in its 2010 report outlining a proposed framework to protect consumer privacy on the internet, the FTC appears, at least for the time being, to have put the onus on the social networks themselves to conduct such a review.[76]

A more formal privacy impact review of privacy policy changes than the one the FTC referred to in its report is necessary. Such a review would benefit both users of social networks and the networks themselves and would also help fill the accountability vacuum resulting from the absence of legal constraints on U.S. online social networks imposing unanticipated changes in their privacy policies. This Note will propose an operating framework for such reviews, and explain why they will help social networking sites strike a better balance between user privacy and web site functionality.

First, to help insure that there is a balance between the privacy needs of users and the business needs of social networking operators, impact reviews of proposed privacy changes on social networks should not be left to the social networks themselves to conduct, but rather be carried out by a government agency.[77] This would ensure that every privacy policy change would be transparent and that users of the networks would be well informed before the change occurs.

While this review could be performed by a new agency, the FTC would be the best choice to perform these reviews, because it already has jurisdiction to regulate privacy in other respects and experience in the field. The benefit of having the FTC conduct an impact review of proposed privacy changes is clear. The FTC is currently the agency in charge of determining violations regarding social network privacy practices, and it has brought a number of cases to enforce the privacy policies of websites.[78]

In order to implement this type of privacy policy review, laws would need to be enacted, vesting the power to conduct this review in a government agency and defining the general class of websites that would fall under the category of "social network" and the scope of the

---

[75] *Protecting Consumer Privacy in an Era of Rapid Change*, FEDERAL TRADE COMMISSION 51 (Dec. 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[76] *See id.* at 51 – 52, 76 – 77.

[77] While this proposal limits the impact review only to social networks, the types of privacy changes conducted by sites such as Facebook are indicative of a larger problem that spans many different types of websites. Due to this, this type of policy review could be used for sites that do not have a social networking function.

[78] *See Enforcing Privacy Promises: Section 5 of the FTC Act*, *supra* note 69.

review itself. Congress should not provide a statutory definition of social network due to the rapid change in the way social networking sites operate and exist. By describing only the general class of websites that would meet the definition, Congress would be giving the FTC broad authority to pinpoint the definitions of what types of sites fall under the classification of a "social networking site." By doing this, the FTC would have the flexibility needed to keep up with the evolving nature of social networking sites.

The process for the impact review should not be too difficult or too lengthy, as this could prompt social networking sites to leave outdated privacy policies unchanged. The social network would first propose the changes it wishes to make, in writing, to the FTC. In this proposal, the social network would be required to detail specifically how and where the privacy policy is being altered. Along with any changes proposed, the social network would be required to document how a proposed change would better the privacy of its users or why a proposed reduction in privacy would not seriously or negatively affect its users.

The proposed changes along with any accompanying material would then be posted online at the FTC's website. The FTC would then allow the public and interested parties to comment on the proposed changes. People would be allowed to provide any comment they wanted regarding the proposed changes. This would all be in an effort to solicit the views of the people using the social networks. Because this process should not be excessively burdensome to social networking sites attempting to alter their privacy policies, the solicitation of comments should not last any longer than reasonably needed in order to obtain comments.

The panel conducting the impact review at the FTC would then, within a reasonable time, review the proposed changes and statements by the proposing social network, read the public comments and concerns and prepare a report outlining its recommendation regarding the proposed changes. This report should summarize public concerns, assess the legitimacy of the social network's need for privacy change, and offer recommendations to the social network of ways to alleviate public concern, if needed.

After this report is issued, the social network would be free to implement its privacy policy as originally proposed, or with alterations in line with the recommendations of the FTC panel. However, the social network would be required to post its proposed changes again, along with the report from the FTC, for a reasonable period before the changes take effect. This period of time should be long enough to allow users to assess the proposed changes. The social network would also be required to allow users, during this period, to cancel their

membership in the network easily and have their information permanently erased.

This process should be mandatory even if social networking websites are not legally required to implement the FTC's recommendations. There are three primary benefits to making the process mandatory. First, social networking sites would be forced to provide greater transparency with regard to the planned privacy changes. Second, social networking sites would be forced to examine the impacts of their privacy policy decisions, thus increasing their own awareness of the possible effects. Last, users would be able to make more efficient market choices because the increased transparency would allow them to "vote with their feet" and leave sites before potentially harmful changes take effect.

It should be stressed, however, that despite the benefits of the process being mandatory, the networks should be given latitude to analyze an FTC report, and make its own business decision about whether to change the proposed policy or implement it as originally planned.[79] This process is ultimately not designed to interfere with the business of social networking but rather to increase the transparency and understanding of the privacy changes that are being made. Additionally, as a possible motivating factor to encourage social networking sites to implement the FTC's suggestions, sites that do can be guaranteed immunity from any potential liability of implementing a policy that has been edited and approved by the FTC. This type of immunity should not be a concern to users who do not agree with implemented privacy policies due to the open nature of the process, which, regardless of the privacy policy that is ultimately put into effect, would allow users to leave social networking sites before the changes take effect.

Having an agency assess the practicality of privacy concerns on social networks in this manner would have many benefits for both the social networks and their users. First and most importantly, such a review system could head off any changes to privacy policy that would be fundamentally detrimental to the users of social networks. This is because the changing of privacy policies would be more open, requiring social networking sites to make their planned changes public, and giving users the opportunity to react to any changes they believe are detrimental to their expected privacy interests.

---

[79] While the privacy impact review is non-binding, it could certainly have some effect against a network if a complaint is later brought against the social networking site after it enacts a policy that goes against recommendation.

Second, establishing a review process for privacy changes on social networks would prevent rapid and drastic privacy changes. This is of obvious benefit to the users of social networks because it will prevent a network from suddenly, and fundamentally, altering the privacy spectrum on the network. Further, this will be a benefit to the social network because it will no longer have to fear the kind of user backlash,[80] or formal complaints,[81] that Facebook has previously received in response to the overhaul of its privacy policy.

Finally, this type of review process would provide the type of transparency needed to actively evaluate any new privacy policy on a social network. This would give users and other interested third parties the opportunity to see the specific changes a social network wishes to make before it actually makes them. Further, transparency would give users the opportunity to comment on the proposed changes, which would prompt meaningful dialogue between the social networks and their users in a manner that may ultimately lead to the development of privacy policies that are optimal for both.[82]

III. CONCERNS AND LIMITATIONS OF PRIVACY POLICY IMPACT REVIEWS

A. USER DISCONNECT AND ITS RAMIFICATIONS ON PRIVACY CHANGE REGULATION

Perhaps the biggest limitation to the efficacy of any governmental review of privacy changes for online social networks is the fact that many users of online social networking sites do not use the privacy protections that are available to them. This danger was clearly illustrated in July of 2010 when a hacker compiled a 2.8GB torrent file containing harvested data of Facebook users who had not bothered to change their privacy settings to make their pages unavailable to search

---

[80] *See* Tracy Samantha Schmidt, *Inside the Backlash Against Facebook*, TIME (Sep. 6, 2006), http://www.time.com/time/nation/article/0,8599,1532225,00.html (2006 Privacy Backlash); David Gelles, *Facebook Retreats After Latest Privacy Row*, FINANCIAL TIMES (Feb. 19, 2009), http://blogs.ft.com/techblog/2009/02/facebook-retreats-after-latest-privacy-row (February 2009 Privacy Backlash); Ryan Singel, *Facebook Loosens Privacy Controls, Sparks a Backlash*, WIRED (Dec. 10, 2009), http://www.wired.com/epicenter/2009/12/facebook-privacy-backlash (December 2009 Privacy Backlash).

[81] *See supra* note 64.

[82] This would hopefully give social networks better insight into the concerns and needs of their users.

engines.[83] This directory contained the information of 100 million individual users.[84] Further, Mark Zuckerberg, the founder of Facebook, recently stated that openly sharing more information with more people has become the social network users' "social norm."[85] He believes that this is because "[p]eople have really gotten comfortable" sharing information.[86] The fact that users of Facebook seemingly do not give much attention to their privacy settings is obviously apparent to Facebook; the problem is that it may not be apparent to the users themselves.

A 2005 study conducted by Ralph Gross and Alessandro Acquisti of Carnegie Mellon University sheds much-needed light on how big an issue is created by social networking users' lack of awareness of their privacy options. This study highlights patterns of information revelation on social networking sites, as well as potential attacks, such as stalking, data mining, and identification.[87] Further, this study shows evidence that a minimal number of users change their default privacy settings.[88] Information was collected in June 2005 from 4540 Facebook profiles of students at Carnegie Mellon University ("CMU").[89] At the time of this study, this was "virtually the entire CMU Facebook population."[90] This information indicated that, of all the collected Facebook users at CMU, 73.7 percent were undergraduates, and that graduate students, staff, and faculty were

---

[83] James Nixon, *100 million Facebook pages leaked on torrent site*, THINQ.CO.UK (July 28, 2010), http://www.thinq.co.uk/2010/7/28/100-million-facebook-pages-leaked-torrent-site.

[84] *Id.*

[85] Bobbie Johnson, *Privacy no longer a social norm, says Facebook founder*, THE GUARDIAN (Jan. 11, 2010) http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

[86] *Id.*

[87] Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks (The Facebook Case)*, ACM Workshop on Privacy in the Electronic Society 71, 71 (2005).

[88] *Id.*

[89] *Id.* at 74.

[90] *Id.*

represented to a much lower extent.[91] The average age of the users collected for data was 21.04 years.[92]

The researchers first sought to evaluate the extent to which users at CMU shared their personal information on Facebook.[93] Their results showed that CMU users shared an "astonishing amount" of Personal Identification Information.[94] 90.8 percent of profiles contained an image, 87.8 percent of users revealed their birth dates, nearly 40 percent shared a phone number, and slightly more than half shared information pertaining to their current residence.[95] The researchers noted that Facebook profiles "tend to be fully identified with each participant's real first and last names."[96] Because of this, anyone who views the profile will be able to connect the information on the profile with the real name of the person who posted it.[97]

The researchers proceeded to assess the validity of the information they collected.[98] They noted that at the time of the study, Facebook required a valid email address from one of the more than 500 colleges open to the site and encouraged users to publish profiles that pertained only to themselves.[99] It should be noted at this point that Facebook now allows anyone with a valid email address to join, but that its current terms of service explicitly require that a user "not provide any false personal information on Facebook, or create an account for anyone other than [the user] without permission."[100]

Using a measurement of "perceived" accuracy, the researchers found that 89 percent of all names were likely to be the true names of

---

[91] *Id.*

[92] *Id.*

[93] *Id.* at 75.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.* at 75-76.

[100] *Statement of Rights and Responsibilities*, FACEBOOK (Dec. 21, 2009), http://www.facebook.com/terms.php.

the individuals using them.[101] It was further found that 98.5 percent of all profiles that included birth date information reported a full date.[102] While it could not be proven that these dates were truthful, the researchers observed posts on some profiles expressing birthday wishes that correlated to the dates given and noted that the incentives to provide a false birth date, when none was required at all, were unclear.[103]

Further, although there was no explicit requirement to post a photo at the time of the study, 90.8 percent of all users in the study did.[104] Of these, 61 percent of the photos were suitable enough to make a direct identification of the person who created the profile.[105]

Next, the study analyzed the actual privacy settings of Facebook users.[106] At the time, Facebook reinforced the default privacy settings, which were the least restrictive, by labeling them "recommended."[107] These settings allowed anyone, regardless of their institutional affiliation, to gain access to a user's full name, profile image, institution, and status at that institution.[108] Additionally, the default settings allowed anyone within a user's institution to see the full profile of the user.[109] The researchers noted that Facebook's choice for default privacy was significant because prior research had shown that "users tend to not change default settings."[110] With regard to the

---

[101] Gross, *supra* note 88, at 76. (The authors concede that it is difficult to determine the accuracy of information posted on social networks. Due to this, when the authors state they are using a method of "perceived accuracy," they are stating that they manually determined, based on their own perceptions of the information, how accurate or truthful it is. For example, when determining the accuracy of names, they sort names into three categories: Real Names, Partial Names, and Obviously Fake Names.).

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *Id.* It should be noted that the options for privacy settings have been changed since this study. Details of more recent changes to Facebook's privacy policy can be found in Part I.

[107] *Id.* at 77.

[108] *Id.*

[109] *Id.*

[110] *Id.*

searchability and visibility of the profiles in their data set, it was concluded that "only a vanishingly small number of users change the (permissive) default privacy preferences."[111]

Because of the ease of access to the profiles of users, it was found that it would be "relatively easy for anybody to gain access to [the data in the profiles], and cheap to store a nation-wide database of fully identified students and their IDs."[112] The privacy implications are profound because such information can be used to "re-identify" other information about users that have been "de-identified," such as by hospital discharge data, by comparing the private information provided by users to other private documents with no identity attached.[113]

Further, by including birthdates, hometowns, current residences, and current phone numbers, users may enable the discovery of their social security numbers ("SSN") and ultimately identity theft.114 As the researchers explain:

> "The first three digits of a social security number reveal where that number was created (specifically, the digits are determined by the ZIP code of the mailing address shown on the application for a social security number). The next two digits are group identifiers, which are assigned according to a peculiar but predictable temporal order. The last four digits are progressive serial numbers.
>
> When a person's hometown is known, the window of the first three digits of her SNN can be identified with probability decreasing with the home state's populousness. When that person's birthday is also known, and an attacker has access to SSNs of other people with the same birthdate in the same state as the target (for example obtained from the SSN death index or from stolen SSNs), it is possible to pin down a window of values in which the two middle digits are

---

[111] *Id.*

[112] *Id.* at 78.

[113] *Id.*

[114] *Id.*

> likely to fall. The last four digits (often used in unprotected logins and as passwords) can be retrieved through social engineering."[115]

Because the vast majority of the profiles analyzed provided the type of information needed for identify theft, the users were exposing themselves to substantial risks.[116] The researchers also point out that even if the profile users were not very concerned about the visibility of their info at the time, a digital dossier of data mined information could be used to identify them for years to come.[117]

Based on the information provided in the CMU research, one might conclude that users of social networks such as Facebook simply do not care about privacy. Facebook founder Mark Zuckerberg believes this notion, stating that privacy is no longer a social norm.[118] If this is indeed true, then no amount of regulation regarding the privacy changes of social networks will likely matter. It is possible, however, that users do not know enough about the ramifications of the amount of information they share; what is missing is not concern, but education.

danah boyd, a Microsoft researcher and social networking expert, is explicitly critical of Zuckerberg's stance. To boyd, privacy isn't dead at all.[119] boyd defines privacy as being able to *control* how information flows:

> "Wanting privacy is not about needing something to hide. It's about wanting to maintain control. Often, privacy isn't about hiding; it's about creating space to open up. If you remember that privacy is about maintaining a sense of control, you can understand why Privacy is Not Dead. There are good reasons to

---

[115] *Id.* at 78 – 79 (citations omitted).

[116] *Id.* at 79.

[117] *Id.*

[118] Johnson, *supra* note 86.

[119] boyd, danah. 2010. "Making Sense of Privacy and Publicity." *SXSW.* Austin, Texas, March 13, *available at* http://www.danah.org/papers/talks/2010/SXSW2010.html.

> engage in public; there always have been. But wanting to be in public doesn't mean wanting to lose control."[120]

This analysis might explain why sites such as Facebook experience enormous backlash from their users when privacy policy changes fundamentally alter the way the users can control their information, as evidenced by the backlash against Facebook when it made information public that users previously had the ability to control.

Further research may support boyd's conclusion that users of social networks have not given up their concern over privacy on the networks. A 2006 study, centered on Facebook, found that, regardless of whether a participant was a member of the social networking site, "[r]espondents were more concerned about threats to their personal privacy than about terrorism or global warming."[121] This finding, which is highly notable, as it came only five years after the attacks of September 11, 2001, at the very least initially indicates that people are still very concerned about personal privacy.

The study further found, not surprisingly, that sensitivity towards privacy is stronger among non-members of Facebook than it is among members.[122] It is not always true, however, that depth of privacy concern prompts resistance to social networking. The researchers found that, among undergraduate students, even those students who expressed the highest level of concern for personal privacy joined Facebook at an amazing rate of 89.74 percent.[123] These results suggested that "[Facebook] membership among undergraduates is *not* just a matter of their not being concerned, in general, about their privacy."[124]

The CMU study suggests that Zuckerberg may be incorrect in his explanation of Facebook users' apparent inattention to privacy. It may not be that privacy indifference is the new "social norm." Even the majority of undergraduates in the study who were concerned about privacy were members of Facebook. As of December 2009, the largest

---

[120] *Id.*

[121] Allesandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on Facebook*, 4258 Lecture Notes in Computer Science 36, 44 (2006).

[122] *Id.* at 45.

[123] *Id.* at 46.

[124] *Id.* at 48.

segment of American Facebook users was the 18-25 age group, comprising 29 percent of the estimated hundred million users in the United States.[125]

It seems far more likely, but admittedly unproven, that the younger generation represented by the undergraduate community perceives being a part of the network as a necessary social norm, regardless of personal concerns over privacy. This perception may be the driving force that compels individuals who are concerned about personal privacy to join a network designed to share personal information. If people feel compelled, however, to join social networks despite concerns over personal privacy, the users of sites such as Facebook will need to take their privacy options seriously after they join the network. Specifically, in order for any regulation of privacy changes on social networking sites to be effective and useful, users of social networking sites will need to take more responsibility for the information that they post online. Protective regulations may be put into effect, but will be of little use if users are not vigilant.

It is clear that the threat of rapidly changing privacy policies on social networking sites is only part of the privacy problem. Members of social networks need to be aware of the options available to them. The public discussion component of this Note's proposal for privacy policy reviews could help address and promote that awareness. FTC public comment opportunities would create a public forum for users to learn about and to discuss the options available to them, which could potentially lead to more informed privacy choices by the users themselves.

B. IS A REVIEW PROCESS NECESSARY IF USERS CAN "VOTE WITH THEIR FEET?"

With all the privacy controversy surrounding Facebook, the most popular social networking site in the world, it stands to reason that privacy-minded alternatives will begin to form. It can be argued that if these new social networking sites offer viable alternatives to users who want greater control over their privacy protections, then there would not be a need for regulation as users would be able to "vote with their

---

[125] Justin Smith, *December Data on Facebook's US Growth by Age and Gender: Beyond 100 Million*, INSIDE FACEBOOK (Jan. 4, 2010), http://www.insidefacebook.com/2010/01/04/december-data-on-facebook's-us-growth-by-age-and-gender-beyond-100-million.

feet."[126] By doing so, users could effectively demonstrate their discontent with a privacy change by leaving the network. While some privacy-minded social networks may be beginning to emerge, it is difficult to see what impact their presence will bring to the issue.

One such potential newcomer is the upcoming social networking site "Diaspora."[127] This site was created by four New York University students who wanted to create a social networking site that they claim values privacy.[128] The creators view Diaspora as the '"privacy aware, personally controlled, do-it-all distributed open source social network."'[129] "[T]he core idea behind Diaspora is that each user will have their own encrypted, customizable 'node' on the Diaspora network. Your personal data live on your computer instead of a centralized hub."[130] The group posted a description of their idea on a website that connects internet donors with underfunded projects and quickly made nearly five times the amount of their original funding goal, demonstrating that there is at least some demand for the group's project.[131]

Another possible newcomer into the social networking business may not be coming from a small startup company, as Google has been the recent subject of speculation regarding a new social networking platform. Google has already admitted that it at least plans to infuse its core products with elements of social networking,[132] although a

---

[126] It does not seem outlandish as recent data suggests that the big social networking sites such as Facebook or Myspace have as much customer satisfaction as airlines and cable companies. *See* Chloe Albanesius, *Facebook, Myspace Get Failing Grade on Customer Satisfaction*, PCMAG.COM (July 20, 2010), http://www.pcmag.com/article2/0,2817,2366730,00.asp.

[127] More info can be found at http://www.joindiaspora.com.

[128] Kyle VanHemert, *Diaspora: The Student-Made, Privacy-Respecting Facebook Alternative*, GIZMODO (May 12, 2010), http://www.gizmodo.com/5537502/diaspora-the-student+made-privacy+respecting-facebook-alternative.

[129] *Id.*

[130] Brian Barret, *This Is What Student-Made Facebook Alternative Diaspora Looks Like*, GIZMODO (Sept. 16, 2010), http://www.gizmodo.com/5639706/this-is-what-the-student+made-facebook-alternative-diaspora-looks-like.

[131] *See supra* note 126. The group set a goal of raising $10,000, but by May of 2010 had raised closer to $50,000.

[132] Amir Efrati, *Google Fired Worker After Customer Breach*, WALL ST. J. (Sept. 24, 2010), http://online.wsj.com/article/SB10001424052748704285104575492440245394392.html.

rumor persists that Google is going to launch a complete social networking service called "Google Me."[133] If true, this could be a viable alternative for privacy-seeking users of social networks, as Google is often well-regarded for its concern for user privacy, which is evidenced by its recent overhaul of its privacy policy in order to make it more transparent and understandable.[134]

It can be argued that if either of these alternatives, or any others, is able to successfully establish a user base, then the market for social networking will be open enough for users to make choices based on how they value their own privacy, alleviating the need for any regulation. However, it is currently unknown how successful any of these sites will be. Further, it is difficult to gauge how a claimed privacy-minded social network would operate in the future. Facebook was once regarded by its users as being privacy-minded and has since been embroiled in controversy after controversy regarding its privacy changes. The need for a simple regulatory scheme that seeks to make privacy changes more transparent, and thus educate and protect the user base, will likely be present no matter how the social networking market evolves in the future.

CONCLUSION

Social networking sites are quickly becoming a commonplace fixture in the daily lives of more and more people.[135] The members of these sites invest a lot of their personal information in order to make the sites function as intended. Protections need to be put into place to both proactively protect users from rapid policy changes and educate the users of social networking sites with transparency in the privacy

---

[133] Tom Krazit, *'Google Me' Google's next social experiment?* CNET NEWS. (June 29, 2010), http://news.cnet.com/8301-30684_3-20009159-265.html.

[134] *Google Simplifies Privacy Policy*, ESECURITYPLANET (Sept. 7, 2010), http://www.esecurityplanet.com/headlines/article.php/3902236/article.htm. Although, it should be noted that Google is not without its own privacy scandals. Google recently settled a class action lawsuit brought by its users over its product "Google Buzz." Buzz is a social networking application found within Google's Gmail service. The idea of Buzz is to create social networks around a user's email contacts. However, when Buzz was implemented it was designed as an opt-out program, initially giving little control over how users were connected to others. The program has since become opt-in. *See* Claudine Beaumont, *Google Settles Buzz Lawsuit for $8.5 million*, THE TELEGRAPH (Sept. 6, 2010, 4:27 PM), http://www.telegraph.co.uk/technology/google/7984903/Google-settles-Buzz-lawsuite-for-8.5-million.html.

[135] *See supra* note 2.

setting process. A reactive solution, focused on punishing social networking sites for unfair business practices, is not optimal because it is likely to come too late to protect the information that sudden changes in a privacy policy may expose. A regulatory review of proposed privacy changes will help social networks strike a better balance between user privacy and network functionality, promote user awareness of both existing policies and options for self-protection, and avoid the alienation of network members who resent sudden changes in the privacy policies on which they have come to rely.